3101/01356

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

#4
3-11-0

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年 １月１０日

出願番号
Application Number: 特願２００２－００２９３５

[ST.10/C]: [ＪＰ２００２－００２９３５]

出願人
Applicant(s): 株式会社日立製作所

CERTIFIED COPY OF
PRIORITY DOCUMENT

U.S. Appln Filed 3-1-02
Inventor: A. Hashimoto et al
mattingly Stanger & Malur
Docket H-1039

２００２年 ２月１５日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号 出証特２００２－３００６９０１

【書類名】　特許願
【整理番号】　H01013561A
【あて先】　特許庁長官　殿
【国際特許分類】　G06F　3/06
【発明者】
【住所又は居所】　東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所中央研究所内
【氏名】　橋本　顕義
【発明者】
【住所又は居所】　東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所中央研究所内
【氏名】　上村　哲也
【特許出願人】
【識別番号】　000005108
【氏名又は名称】　株式会社　日立製作所
【代理人】
【識別番号】　100075096
【弁理士】
【氏名又は名称】　作田　康夫
【電話番号】　03-3212-1111
【手数料の表示】
【予納台帳番号】　013088
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　セキュリティ機構を備えた二次記憶装置およびそのアクセス制御方法

【特許請求の範囲】

【請求項１】

複数の不揮発性データ格納手段と、該不揮発性データ格納手段の制御装置と、前記不揮発性データ格納手段と前記制御装置とを相互に接続する内部ネットワークとを有する二次記憶装置において、

前記制御装置は、各々異なるネットワークに接続される複数のネットワーク通信ポートと、前記通信ポートに要求された入出力命令を処理するアクセス制御部と、前記複数の通信ポートの１と前記複数の不揮発性データ格納手段の１との間で許可される入出力命令を規定するアクセス制御設定情報が格納されたアクセス制御テーブルとを有することを特徴とする二次記憶装置。

【請求項２】

請求項１に記載の二次記憶装置において、前記アクセス制御部は、前記アクセス制御設定情報に基づき、前記通信ポートに要求された入出力命令の許可、拒否を判定することを特徴とする二次記憶装置。

【請求項３】

請求項１に記載の二次記憶装置において、前記アクセス制御設定情報は、と前記複数の不揮発性データ格納手段に対して設定された論理ディスクと前記複数の通信ポートの１との間で許可される入出力命令に対して設定されていることを特徴とする二次記憶装置。

【請求項４】

請求項１に記載の二次記憶装置において、前記アクセス制御設定情報を設定、変更する管理コンソールを備えたことを特徴とする二次記憶装置。

【請求項５】

請求項１に記載の二次記憶装置において、全ての通信ポートに対して読出し不許可と設定されたアクセス制御設定情報を備えたことを特徴とする二次記憶装置。

【請求項６】

請求項３に記載の二次記憶装置において、前記アクセス制御部は、不許可と判定した入出力命令を前記管理コンソールに対して報告することを特徴とする二次記憶装置。

【請求項７】

請求項５に記載の二次記憶装置において、前記管理コンソールは、アクセス制御部から報告された前記入出力命令を記録する記録手段を備えたことを特徴とする二次記憶装置。

【請求項８】

各々異なるネットワークに接続される複数のネットワーク通信ポートと、前記通信ポートに要求された入出力命令を処理するアクセス制御部と、前記複数の通信ポートの１と前記複数の不揮発性データ格納手段の１との間で許可される入出力命令を規定するアクセス制御設定情報が格納されたアクセス制御テーブルとを備えた制御装置と、複数の不揮発性データ格納手段と、該不揮発性データ格納手段と前記制御装置とを相互に接続する内部ネットワークとを備えた二次記憶装置のアクセス制御方法において、

前記アクセス制御部は、

前記ネットワーク通信ポートに到着した入出力命令に対して、該入出力命令が対象とする前記不揮発データ格納手段の管理単位と該入出力命令が要求されたネットワーク通信ポートとを同定し、

前記アクセス制御テーブルを参照し、

前記入出力命令が到達した通信ポートと前記入出力命令が対象とする管理単位間で許可されている入出力命令を検索し、

前記入出力命令が許可されているか否かを判定することを特徴とする二次記憶装置のアクセス制御方法。

【請求項９】

請求項８に記載のアクセス制御方法において、前記アクセス制御手段が不許可と判定した場合に、前記入出力命令の送信元に不許可の判定を送信することを特徴とするアクセス制御方法。

【請求項１０】

請求項８に記載のアクセス制御方法において、前記不揮発性データ格納手段に格納された特定のデータに対するアクセス不許可の判定回数が所定の閾値を越えた場合に、前記複数の通信ポートから当該データへのアクセスを不許可とすることを特徴とするアクセス制御方法。

【請求項１１】

請求項８に記載のアクセス制御方法において、前記不揮発性データ格納手段に格納された特定のデータに対するアクセス不許可の判定回数が所定の閾値を越えた場合に、当該二次記憶装置の管理者にアクセス不許可の判定回数が所定の閾値を越えたことを通知するアクセス制御方法。

【請求項１２】

請求項８に記載のアクセス制御方法において、前記入出力命令体系がSCSI（Small Computer System Interface）規格であった場合に、異常の報告として「CHECK CONDITION」ステータスを送信することを特徴とするアクセス制御方法。

【請求項１３】

請求項１２に記載のアクセス制御方法において、ホストコンピュータが「CHECK CONDITION」ステータスを受信した後「REQUEST SENSE」要求を発行した場合に、その応答であるセンス・キー、センス・データとして異常を示すコードを送信することを特徴とするアクセス制御方法。

【請求項１４】

請求項１３に記載のアクセス制御方法において、センス・キーとして「Illegal Request」を送信することを特徴とするアクセス制御方法。

【請求項１５】

請求項１３に記載のアクセス制御方法において、センス・キーとして「Data Protected」を送信することを特徴とするアクセス制御方法。

【請求項１６】

請求項８に記載のアクセス制御方法において、前記入出力命令体系がNFS(Network File System)であった場合に、アクセス不許可の報告として、NFSエラーコード「NFSERR_PERM」を送信することを特徴とするアクセス制御方法。

【請求項１７】

請求項８に記載のアクセス制御方法において、前記入出力命令体系がNFS(Network File System)であった場合に、アクセス不許可の報告として、NFSエラーコード「NFSERR_ACCS」を送信することを特徴とするアクセス制御方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワークに接続された二次記憶装置(ディスク装置)におけるデータの機密性の保持に関する。

【０００２】

【従来の技術】

近年、磁気ディスク装置に代表される二次記憶装置は、ネットワーク志向を強めており、多くの大学や企業で二次記憶装置をLAN(Local Area Network)等のネットワークに直結する技術が開発されている。

二次記憶装置がネットワークに直接接続されるようになると、不特定多数のホストコンピュータがアクセスを行う可能性がある。従って、ネットワークと二次記憶装置間でのデータの機密性の確保、即ち何らかのセキュリティ機構が二次記憶装置側に必要となる。

特開平10-333839（以下、公知例1）には、セキュリティ機構を実装した二次記憶装置の例が開示されている。公知例1のセキュリティ機構では、登録されたホストコンピュータの識別子（公知例1では、World Wide Name）を用いてホストコンピュータの認証を行っている。ホストコンピュータは、二次記憶装置に対する接続要求の際に前記World Wide Nameを二次記憶装置側に送信する。二次記憶装置は、送信されてきたWorld Wide Nameが登録されていれば処理を続行し、登録されていなければ接続拒否応答を行う。

しかしながら、公知例1の方式をネットワークに存在する不特定多数のホストコンピュータに対して適用すると、登録作業が膨大になり管理者の負担は非常に大きなものとなる。従って、ネットワーク直結型の二次記憶装置に対しては、公知例1の方式は現実的には適用が困難である。

更に、登録される識別子は偽造される可能性がある。また、二次記憶装置に対し

て正当な権限を持つ（即ち登録された識別子を有する）ホストコンピュータが侵入を許してしまうと、データの改ざんを防げない。なぜなら、侵入されたホストコンピュータは該二次記憶装置に対して正当な権限を持っているからである。

従来は、不特定多数のホストコンピュータが二次記憶装置に接続される構成は一般的でなく、ユーザ認証等のセキュリティ措置をホストコンピュータ側で行っていたため、従来の二次記憶装置では、ホストコンピュータからの不正侵入による二次記憶装置内のデータの破壊、漏洩を防止することはできなかった。例えば、2000年初頭には、管理者権限を不正に取得した侵入者が、日本政府機関のWebサーバの二次記憶装置内にあるWebページ用ファイルを改ざんする事件が発生した。管理者は正当な権限を持っているため、ホストコンピュータ側からの二次記憶装置内への不正進入を二次記憶装置側で止めることはできない。

成りすましに関しては、ファイアウォールによってある程度防護することができる。ファイアウォールは、それぞれ、インターネットへの接続用、イントラネットへの接続用、非武装地帯（DeMilitarized Zone）接続用と3つのネットワーク通信ポートを持つ。ここで非武装地帯とは、インターネットからのアクセスを受け付ける専用のホストコンピュータを配置した領域である。イントラネット内のホストコンピュータがインターネットからのアクセスを直接受け付けると不正侵入の確率が大きくなるため非武装領域が設けられる。

ファイアウォールは、管理者の定めた規則に従って通信ポートを通過するパケットの通過、不通過を決定する。例えば、通信ポートを通過するパケット内の送信元IPアドレスと当該パケットが入ってきたネットワーク通信ポートとを比較する。当該パケットがインターネット側から入ってきたパケットである場合は、送信元IPアドレスがイントラネット内のアドレスであっても通過させない。IPアドレスが偽造された可能性が高いためである。また、ファイアウォールを設けることにより、外部からのアクセスが非武装地帯に限定されることになるため、重要なデータが存在するイントラネットへの侵入の確率も低下する。

【０００３】

【発明が解決しようとする課題】

上述のとおり、公知例1の方式ではホストコンピュータの権限を不正に取得した

侵入者の二次記憶装置への侵入を防止できない。これは、公知例1が、ホストコンピュータからの送信情報によってアクセス制御する点と、接続許可、拒否の2通りの選択肢しか持っていない点に起因する。ホストコンピュータからの送信情報は、偽造の可能性がある。また、接続許可、拒否の2通りの選択肢しか持っていないと、一旦接続を許可すればどんな作業も許してしまうからである。
また、ファイアウォールで行っていることはパケットの通過、不通過の判定のみであるため、ファイアウォールでは二次記憶装置に対するアクセス種別に応じたきめ細かな保護を行うことはできない。ネットワーク直結型の二次記憶装置においては、二次記憶装置は不特定多数のホストコンピュータに接続される。パケットの通過、不通過の判定規則は、接続されるホストコンピュータが増加するに連れて複雑になる。従って、ネットワーク直結型の二次記憶装置向けのデータ保護という観点では、ファイアウォールは適切な防御法とは言えない。

【０００４】

そこで、本発明が解決しようとする課題は、ネットワーク直結型の二次記憶装置に適したセキュリティ保護方法を提供することにある。

【０００５】

【課題を解決するための手段】

本発明では、二次記憶装置に複数のネットワーク通信ポートを持たせて、通信ポートをそれぞれ異なるネットワークに接続する。アクセス要求の接続許可、不許可の判定は、二次記憶装置内のデータに対する入出力命令（例えば、読み込み、書き込み）というアクセス種別単位で行い、この判定をネットワーク通信ポートごとに行う。
ネットワーク通信ポートへのアクセス要求に対して、読み込み、書き込みというアクセス種別単位で許可、不許可を設定するため、ホストコンピュータへ不正侵入されてもデータが改ざんされることは無くなる。また、ネットワークの物理構成をもとに許可、不許可を判定するため、成りすまし攻撃が通用しない。更に、ホストコンピュータを識別するのではなく、ホストコンピュータの属するネットワークを識別して、許可、不許可を判定するために、管理者の運用負担が大きく軽減される。

【０００６】

【発明の実施の形態】

以下図面を用いて、本発明の実施の形態を説明する。

（実施例１）

本発明の構成例を図1に示す。本実施例では、二次記憶装置として磁気ディスク装置を用いて発明の実施の形態を説明する。磁気ディスク装置101は、磁気ディスク制御装置102と、実際にデータを格納する磁気ディスク駆動装置103、104、105と、前記磁気ディスク制御装置102と磁気ディスク駆動装置103、104、105を接続する内部ネットワーク106からなる。図1では、内部ネットワークが円状の形態を持っているが、本発明が内部ネットワークの形態に依存しないことはいうまでもない。

磁気ディスク装置101は、ネットワーク１(107)とネットワーク２(108)と接続されている。ネットワーク１(107)には、ホストコンピュータ108、109が、ネットワーク1008には、ホストコンピュータ110、111が接続されている。ここでいうネットワークとは、IP(Internet Protocol)技術で想定される管理単位である。インターネットに代表されるWAN(Wide Area Network)には、さまざまに企業、団体が参加している。企業、団体にも内部でネットワークを敷設しており、WANは階層的な構造をもっている。この階層的な構造の1つの単位が本実施例でいうネットワークである。異なるネットワーク間には、必ず1か所接続点がある。この接続点で通信を中継する機器をゲートウェイ、ルータという。異なるネットワーク間の通信にはゲートウェイを通過しなくてはならないが、ゲートウェイには前記ファイアウォールも同時に設置してあり、不正な侵入は難しい。

磁気ディスク制御装置102は、ホストコンピュータ109～112から要求のあった入出力命令を受信、解釈し、適切な形に変換して磁気ディスク駆動装置103～105に発行する。ホスト側通信ポート０(113)、ホスト側通信ポート１(114)は、ホストコンピュータ側のネットワークの通信を制御する。アクセス制御部115、116は、ホスト側通信ホストコンピュータ109～112からの要求を解釈、実行する。ディスク側通信制御部117、118は、内部ネットワーク106との通信制御を行う。データ転送制御部119、120は、入出力処理で発生するデータ転送時に、ホスト側通信ポ

ート０(113)とホスト側通信ポート１(114)とディスク側通信制御部117、118の間のデータ転送を行う。内部バス121、122は、ホスト側通信ポート０(113)、ホスト側通信ポート１(114)、アクセス制御部115、116、データ転送制御部119、120を相互接続する。アクセス制御テーブル123は、磁気ディスク駆動装置103～105に記憶されたデータのアクセス権限設定情報を格納する。管理コンソール124は、管理者が磁気ディスク装置101の保守、管理を行うための情報表示、保守要求の送受信に使用する。管理コンソール124は、情報表示のための画面(図示せず)や、管理者からの要求を受け付けるキーボードのような入出力機器(図示せず)を備えている。また管理コンソール124は、磁気ディスク装置101と物理的に一体化しており、構成変更、電源切断、電源投入などのシステムに重大な影響のある操作は、装置の前に立たなければできないようになっている。これは、装置の前に立つということが侵入者にとって最も困難なチェックポイントであるからである。テーブル制御部125は、管理コンソールと通信して、アクセス制御テーブル123の内容を管理コンソールに転送したり、変更したりする。図1では、ホスト側通信ポートが2個搭載しているが、本発明は、ホスト側通信ポートの数に依存しないことはいうまでもない。

図2にアクセス制御テーブル123の形式と設定例を示す。論理ディスク０(201)、論理ディスク１(202)、論理ディスク(n-1)(203)の列は、論理ディスクごとのアクセス権限設定を記述する。ここで論理ディスクとは、磁気ディスク制御装置102がホストコンピュータ109～112に対して仮想的に実現した磁気ディスクである。論理ディスクは、磁気ディスク駆動装置103～105と一致してもよいし、一致していなくてもよい。論理ディスクの利点は、実際に搭載した磁気ディスク駆動装置の記憶容量に依存せず、容量を設定できるなど、管理面の自由度が高くなる点である。通信ポート0 204の行は、ホスト側通信ポート０(113)からのアクセスが各論理ディスクに対して許可された入出力命令が記述される。通信ポート1 205の欄も同様である。このようにして、アクセス制御テーブル123の各欄は、論理ディスクに対して、通信ポートからの許可された入出力命令を記述する。記述できるのは、「READ可能」、「WRITE可能」、「-」の3種類である。「READ可能」はREADのみ可能、「WRITE可能」はWRITEのみ可能、「-」は、当該通信ポートに

接続されたホストコンピュータは検出できない。従来のセキュリティ技術は、ネットワーク接続の許可、拒否のレベルで制御していたため、アクセス制御テーブルの各欄に「READ WRITE可能」か「-」しか記入できないことに相当する。

図2では、論理ディスク0は、通信ポート0からのアクセスはREAD WRITE可能であるが、通信ポート1からはREADのみ可能であることを示している。論理ディスク1は、通信ポート0からはREAD WRITE可能、通信ポート1からは検出不能である。すなわち通信ポート1 114に接続したホストコンピュータ111～112は、論理ディスク1の存在さえわからない。論理ディスク(n-1)は、逆に通信ポート0からは検出不能だが、通信ポート1からはREAD WRITE可能である。

本実施例では、許可する入出力命令を「READ」、「WRITE」としたが、データに対する可能な入出力命令に対して拡張可能なのはいうまでもない。たとえば、二次記憶装置インタフェースの代表的な規格であるSCSI規格では、数十種の入出力命令を規定しており、前記SCSI規格の入出力命令それぞれをアクセス制御テーブル123の各欄に記述することも可能である。

さらに、本実施例では、論理ディスク単位でアクセス権限の設定を行うようにしているが、その他のデータの管理単位、たとえば、ファイル、レコード単位でのアクセス権限設定が可能であることはいうまでもない。

図3に磁気ディスク装置101が入出力命令を受信、実行するフローチャートを示す。

ステップ301　処理の開始

ステップ302：ホストコンピュータからの入出力命令はネットワークを介してホスト側通信ポート113または114に到着する。ホスト側通信ポート113または114は、対応するアクセス制御部115、116に入出力命令を転送する。

ステップ303：アクセス制御部115、116は入出力命令に含まれる論理ディスク番号を抽出する。本実施例のように論理ディスク単位で管理する入出力体系では、入出力命令に論理ディスク番号が含まれる。さらに、当該入出力命令が到着したホスト側通信ポートの識別子を取得する。

ステップ304：アクセス制御部115または116は、テーブル制御部125を介してアクセス制御テーブル123を検索する。ステップ303で取得した論理ディスク番号とホ

スト側通信ポート識別子から、アクセス制御テーブル123の該当する欄の内容を読み取る。

ステップ305：アクセス制御部115、116は、アクセス制御テーブル123の該当する欄を読み取った結果、当該入出力命令が許可されているか判定する。

ステップ306：当該入出力命令が許可されていれば、そのまま実行する。

ステップ307：当該入出力命令が許可されていなければ、アクセス制御部115、116は当該入出力命令の失敗をホストコンピュータに通知する。SCSI規格では、入出力命令が失敗すると、ホストコンピュータは、装置のエラー情報を磁気ディスク装置101に要求する「REQUEST：SENSE」要求を発行することがある。磁気ディスク装置101は、「REQUEST：SENSE」要求の応答として、当該要求が許可されていないことをホストコンピュータに送信する方法も可能である。

ステップ308：アクセス制御部115、116は、不正アクセスがあったことを管理コンソール124に報告する。管理コンソール124は、本不正アクセスをログファイルに記録する。

ステップ309：管理コンソール124は、画面に不正アクセスがあったことを表示し、管理者に不正アクセスの発生を伝える。

ステップ310：処理の終了

このようにして、通信ポートごとに、アクセス制御を行うことができる。

アクセス制御テーブル123の情報設定、変更方法を図4に示す。

ステップ401：処理の開始

ステップ402：管理者は磁気ディスク装置101の管理コンソール124の前に立ち、管理コンソール124を操作する。管理者はアクセス制御テーブル123の変更要求を出す。

ステップ403：管理コンソール124は、ステップ402で変更要求を発行した人間が正規の権限を持った管理者か判定する、認証作業を行う。認証の方法は、パスワードによる方法や、指紋、網膜の血管の模様、手の指先の静脈のパターンなどのバイオメトリックスによる方法がある。ただし、本発明は認証の方法に依存しないことはいうまでもない。

ステップ404：ステップ403の認証作業の結果、正規の権限を持った管理者か判定

を行う。

ステップ405：認証作業の結果、管理コンソール124が正規の権限をもった管理者であると認めた場合、管理コンソール124は、テーブル制御部125にテーブル変更要求をだす。テーブル制御部125は、要求に従いアクセス制御テーブル123の当該個所を変更する。

ステップ406：変更が終了したら、テーブル制御部125は管理コンソール124に変更終了を報告する。管理コンソール124は画面に一連の操作が終了したことを表示する。

ステップ407：ステップ404で正規の権限をもっていないと判定された場合、管理コンソール124は画面に正規の権限をもっていないことを表示する。さらに、認証に失敗したことをログファイルに記録する。認証の失敗が短時間のうちに多数発生した場合は、管理コンソールは、人間からの入力受付を停止する措置を取る。

ステップ408：処理の終了

（実施例２）

次に、図5、図6を用いて本発明の第2の実施例を説明する。実施例2は本発明を部門間で磁気ディスク装置101を共有するシステムに適用した例である。複数の部門間で磁気ディスク装置を共有した場合、他部門に対して、読み込みのみ許すデータと、読み込み、書き込み両方許すデータと、存在を全く知らせないデータの3種類がある。本発明を適用すれば、容易にこのような使い分けを実現できる。

磁気ディスク装置101は部門1ネットワーク501と部門2ネットワーク502と接続されている。部門1ネットワーク501には、部門1の人間が使用するホストコンピュータ503、504が接続されている。ホスト側通信ポート０(113)は部門1ネットワーク501に、ホスト側通信ポート1 113は部門2ネットワーク502に接続する。部門2ネットワーク502には、部門2の人間が使用するホストコンピュータ505、506が接続されている。管理者は、磁気ディスク装置101内に論理ディスク0　507～論理ディスク4 511を配置する。

論理ディスク0　507と論理ディスク1 508は、部門1のディスク領域512とする。部門1からはREAD、WRITEともに可能とする。論理ディスク2 509と論理ディスク3

510は部門2のディスク領域513とする。部門2からはREAD、WRITEともに可能とする。論理ディスク4 512は、部門1、2共有領域514とする。すなわち、部門1、2からREAD、WRITE可能とする。さらに、部門1ディスク領域512は、部門1占有領域515と他部門共有領域516に分ける。部門1占有領域515は、他部門からは検出不能とする。他部門共有領域516は、他部門からはREADのみ可能とする。部門2ディスク領域513も同様に、部門2占有領域518と他部門共有領域517に分ける。

このような使い分けを実現するためには、アクセス制御テーブル123を図6のように設定する。論理ディスク0の欄601は、通信ポート0 204の行は「READ可能」、「WRITE可能」の両方を記入する。一方、通信ポート1 205の行は、「-」を記入する。こうして論理ディスク0 507は部門1からはREAD、WRITE可能、部門2からは検出不可とすることができる。論理ディスク1の欄602は、通信ポート0 204の行は「READ可能」、「WRITE可能」の両方を記入する。一方、通信ポート1 205の行は、「READ可能」を記入する。こうして、論理ディスク1 508は、部門1からはREAD、WRITE可能、部門2からは、READのみ可能とすることができる。部門2のディスク領域513に属する論理ディスク2 509、論理ディスク3 510も同様である。部門間共有領域514に属する論理ディスク4　511は、論理ディスク4　605の列内の欄すべてに「READ可能」、「WRITE可能」を記入する。このような設定で両部門からREAD、WRITE可能な領域を作成できる。このようにして部門間のデータ共有と適切なセキュリティ設定が容易に実現できる。

（実施例３）

次に、図7、8を用いて、本発明第3の実施例を説明する。図7は典型的なWebサーバシステムを示したものである。システムはインターネット701に接続され、インターネット701にはWebシステムを利用するクライアント702が接続されている。インターネット701との接続点にはファイアウォール703があり、通信の中継を行っている。ファイアウォール703は、イントラネット704と非武装地帯705に接続されている。非武装地帯705は、【従来の技術】で述べたように、Webサーバ706のようなインターネット701からのアクセスを受けるサーバを限定する目的で設定される。ファイアウォール703がインターネット側から到着するパケットを非武装地帯705側のみに中継することで実現される。イントラネット704には、磁気

ディスク装置101内のデータベースをアクセスするDBサーバ707や、動的なWebページを生成したり、クライアント702に対話的なサービスを提供するAPサーバ708が接続している。近年の対話的サービスを提供するWebシステムでは、Webサーバ706、DBサーバ707、APサーバ708に機能分担するのが一般的になっている。

磁気ディスク装置101は、イントラネット704とWebサーバ706に接続されている。本実施例では、ホスト側通信ポート０(113)をイントラネット704に、ホスト側通信ポート１(114)をWebサーバ706に接続する。磁気ディスク装置101内をインターネット領域709とイントラネット領域710に分割する。

インターネット領域709は、論理ディスク5 711からなり、主にWebページのファイルを格納している。これらは利用者に表示するだけであり、改ざんを防ぐ意味からも、Webサーバ706側からはREADのみ可能とする必要がある。一方、Web管理者は更新作業を行うため、イントラネット704側からはREAD、WRITE可能とする必要がある。

イントラネット領域710は、論理ディスク6 712からなり、主に利用者データベースを格納している。これらはイントラネット704側ではREAD、WRITE可能でなければならないが、インターネット701側からは決してアクセスさせてはならない。したがって、検出不可としなければならない。

本発明を応用すれば、前記設定も容易に実現できる。図8にアクセス制御テーブル123の本実施例における設定を示す。論理ディスク5の列801は、通信ポート0 204の欄は、「READ可能」、「WRITE可能」の両方を設定する。一方通信ポート1 205の欄は、「READ可能」のみ設定する。論理ディスク6の列802は、通信ポート0 204の欄は「READ可能」、「WRITE可能」であるが、通信ポート1 205の欄は「-」を設定する。図8の設定により、Webページ改ざんを防ぎ、イントラネット704側からは随時更新が可能となる。Webページを改ざんするためには、イントラネット704に侵入しなければならないが、ファイアウォール703のような防壁が存在するため、Webサーバ706に侵入するよりも困難になる。

（実施例４）

本発明の第４の実施例は，2つのネットワーク通信ポートをそれぞれ異なるネットワークに接続し，データを2つの領域に分け，該第1のネットワーク通信ポー

トからは，該2つのデータ領域に対して，参照，更新可能とし，該第2のネットワーク通信ポートからは，該第1のデータ領域はいかなるアクセスも不許可，該第2のデータ領域は参照のみ許可する設定を行うことを特徴とするアクセス制御方法にある。

また、2つのネットワーク通信ポートをそれぞれ異なるネットワークに接続し，データを2つの領域に分け，該第1のネットワーク通信ポートからは，該2つのデータ領域に対して，参照，更新可能とし，該第2のネットワーク通信ポートからは，該第1のデータ領域はいかなるアクセスも不許可，該第2のデータ領域は参照，更新可能する設定を行うことを特徴とするアクセス制御方法にある。

【０００７】

【発明の効果】

上記のように、本発明では、ネットワークの物理的配置の情報をもとにデータへのアクセスを制御するため、従来のセキュリティ方式と比較してデータの機密性を高めることができる。

また、従来のようにホストコンピュータ1台1台を認証するのではなく、同一ネットワークに接続したホストコンピュータはすべて同一の権限を持たせるため、管理者の運用負担を減らすことができる。

さらに、二次記憶装置側で入出力命令ごとに許可、不許可の設定が可能なため、データ共有におけるきめ細かい権限設定が可能となる。従来は防げなかったデータの改ざんなどを防ぐことができる。

【図面の簡単な説明】

【図１】

本発明の第1の実施例における全体の構成図である。

【図２】

本発明のアクセス制御テーブルの形式である。

【図３】

本発明の磁気ディスク装置における入出力時のフローチャートである。

【図４】

本発明の磁気ディスク装置におけるアクセス制御テーブル更新、設定時のフロー

チャートである。

【図５】

本発明の第2の実施例における全体の構成図である。

【図６】

本発明の第2の実施例におけるアクセス制御テーブルの内容である。

【図７】

本発明の第3の実施例における全体の構成図である。

【図８】

本発明の第3の実施例におけるアクセス制御テーブルの内容である。

【符号の説明】

101・・・磁気ディスク装置、102・・・磁気ディスク制御装置、103、104、105・・・磁気ディスク駆動装置、106・・・内部ネットワーク、107・・・ネットワーク1、108・・・ネットワーク2、109、110、111、112・・・ホストコンピュータ、113・・・ホスト側通信ポート0、114・・・ホスト側通信ポート1、115、116・・・アクセス制御部、117、118・・・ディスク側通信制御部、119、120・・・データ転送制御部、121、122・・・内部バス、123・・・アクセス制御テーブル、124・・・管理コンソール、125・・・テーブル制御部、201・・・論理ディスク0の欄、202・・・論理ディスク1の欄、203・・・論理ディスク(n-1)の欄、204・・・ホスト側通信ポート0の行、205・・・ホスト側通信ポート1の行、301・・・処理の開始、302・・・磁気ディスク装置101がホストコンピュータから入出力命令を受信するステップ、303・・・アクセス制御部115、116が入出力命令から論理ディスク番号を抽出、該入出力命令を受信した通信ポート識別子を抽出するステップ、304・・・アクセス制御部115、116がアクセス制御テーブルを検索するステップ、305・・・アクセス制御部115、116が当該要求が許可されているか判定するステップ、306・・・アクセス制御部が、当該入出力命令を実行するステップ、307・・・アクセス制御部115、116が当該入出力命令の失敗をホストコンピュータに報告するステップ、308・・・アクセス制御部115、116が管理コンソール124に不正アクセスが発生したことを報告するステップ、309・・・管理コンソール124が画面に不正アクセスの発生を表示するステップ、310・・・処理の

終了、401・・・処理の開始、402・・・管理者がアクセス制御テーブルの変更要求をだすステップ、403・・・管理者を認証するステップ、404・・・正規の管理者か判定するステップ、405・・・アクセス制御テーブルを変更するステップ、406・・・アクセス制御テーブル変更完了を報告するステップ、407・・・権限がないことを表示するステップ、408・・・処理の終了、501・・・部門1ネットワーク、502・・・部門2ネットワーク、503、504、505、506・・・ホストコンピュータ、507・・・論理ディスク0、508・・・論理ディスク1、509・・・論理ディスク2、510・・・論理ディスク3、511・・・論理ディスク4、512・・・部門1ディスク領域、513・・・部門2ディスク領域、514・・・部門間共有領域、515・・・部門1占有領域、516・・・他部門共有領域、517・・・他部門共有領域、518・・・部門2占有領域、601・・・論理ディスク0の欄、602・・・論理ディスク1の欄、603・・・論理ディスク2の欄、604・・・論理ディスク3の欄、605・・・論理ディスク4の欄、701・・・インターネット、702・・・クライアント、703・・・ファイアウォール、704・・・イントラネット、705・・・非武装地帯、706・・・Webサーバ、707・・・DBサーバ、708・・・APサーバ、709・・・インターネット領域、710・・・イントラネット領域、711・・・論理ディスク5、712・・・論理ディスク6、801・・・論理ディスク5の欄、802・・・論理ディスク6の欄。

【書類名】図面

【図１】

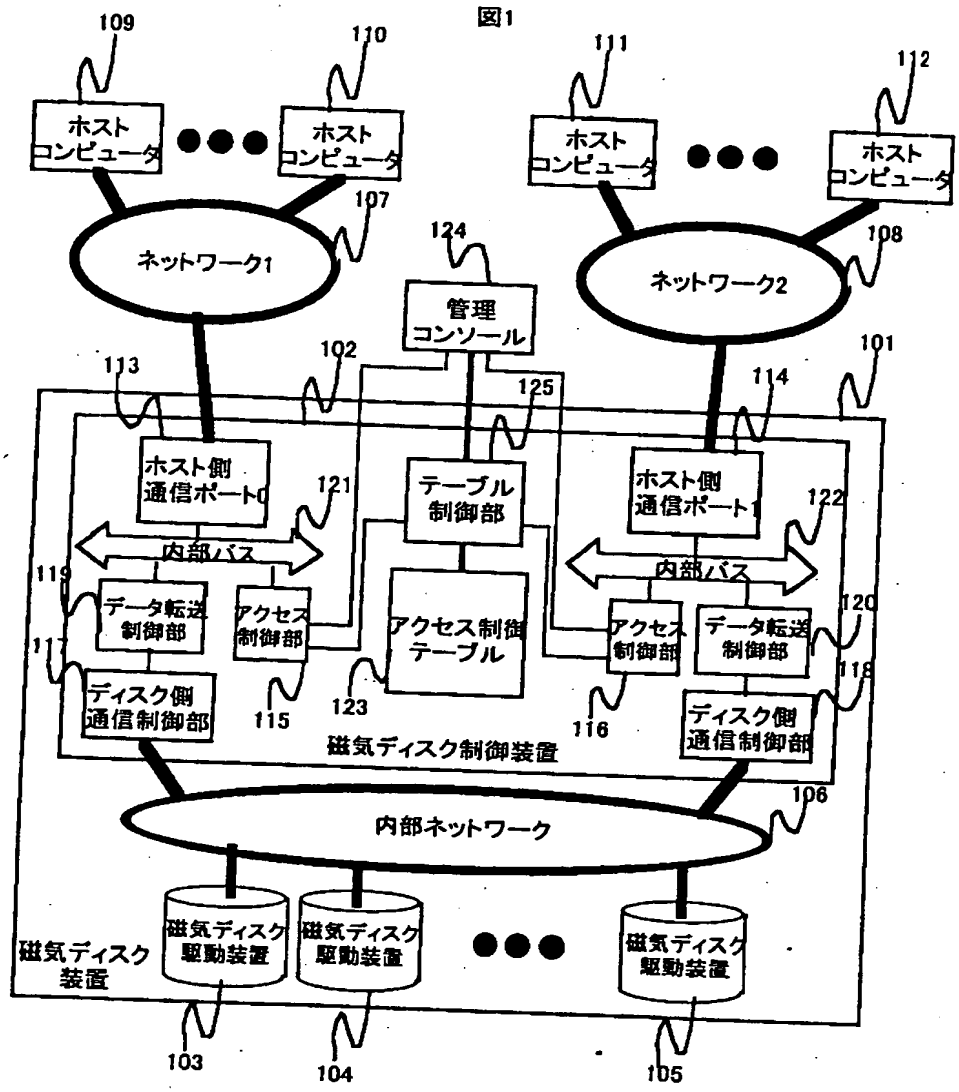
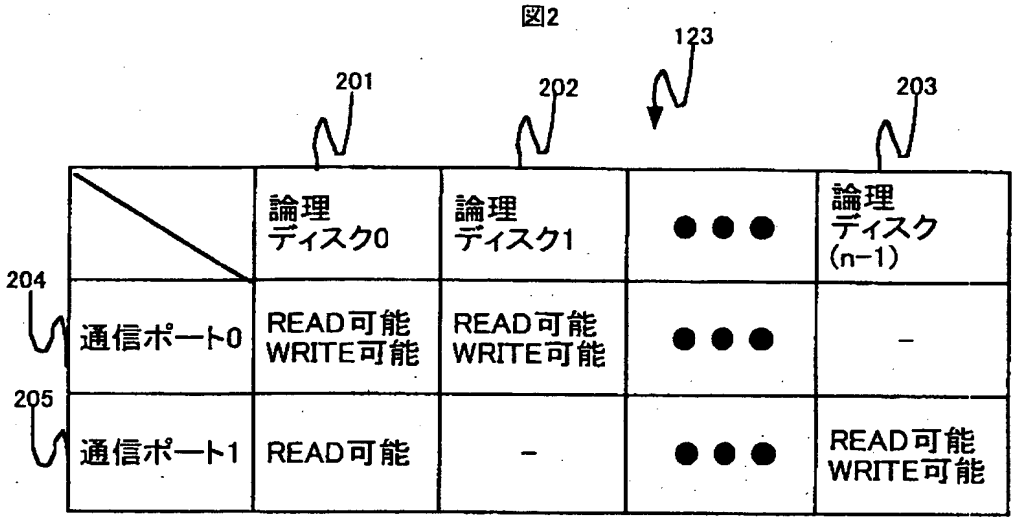


図1
109
110
111
112
ホスト
コンピュータ
ホスト
コンピュータ
ホスト
コンピュータ
ホスト
コンピュータ
107
ネットワーク1
124
管理
コンソール
ネットワーク2
108
102
101
113
125
114
ホスト側
通信ポート0
テーブル
制御部
ホスト側
通信ポート1
121
122
内部バス
内部バス
119
データ転送
制御部
アクセス
制御部
アクセス制御
テーブル
アクセス
制御部
データ転送
制御部
120
117
118
ディスク側
通信制御部
115
123
116
ディスク側
通信制御部
磁気ディスク制御装置
106
内部ネットワーク
磁気ディスク
装置
磁気ディスク
駆動装置
磁気ディスク
駆動装置
磁気ディスク
駆動装置
103
104
105

【図２】

図2



凡例:
READ可能: READのみ可能
WRITE可能:WRITEのみ可能

【図３】

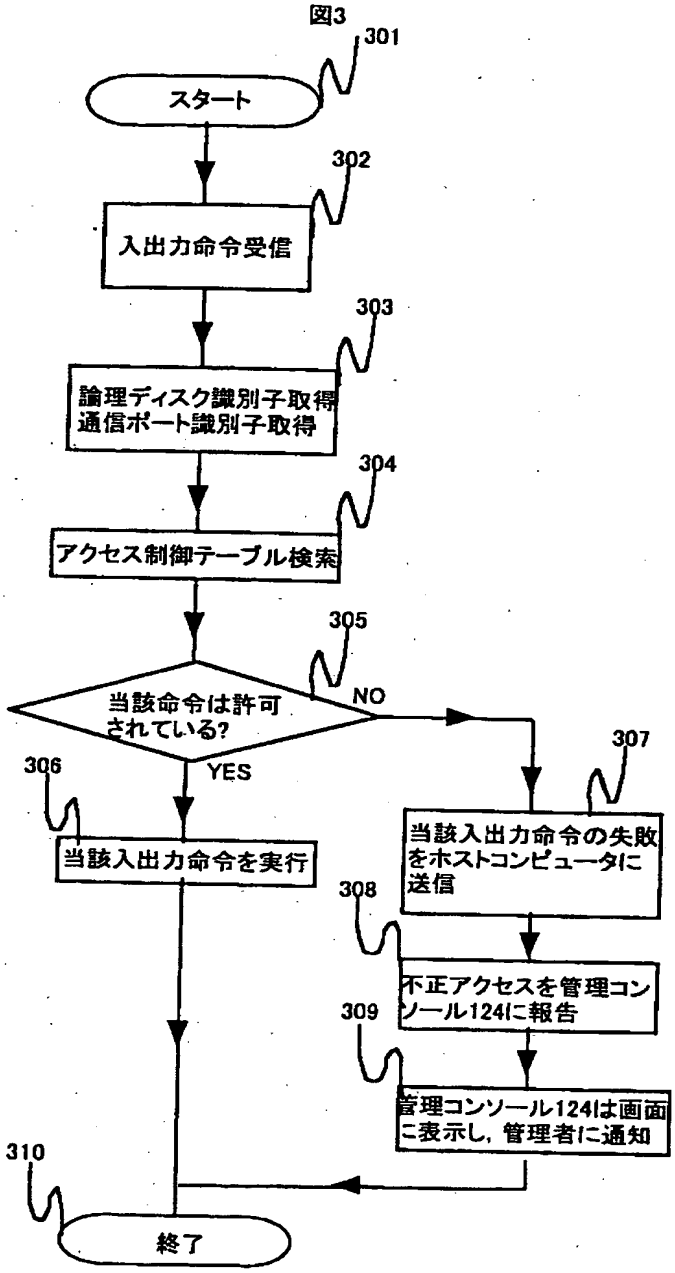
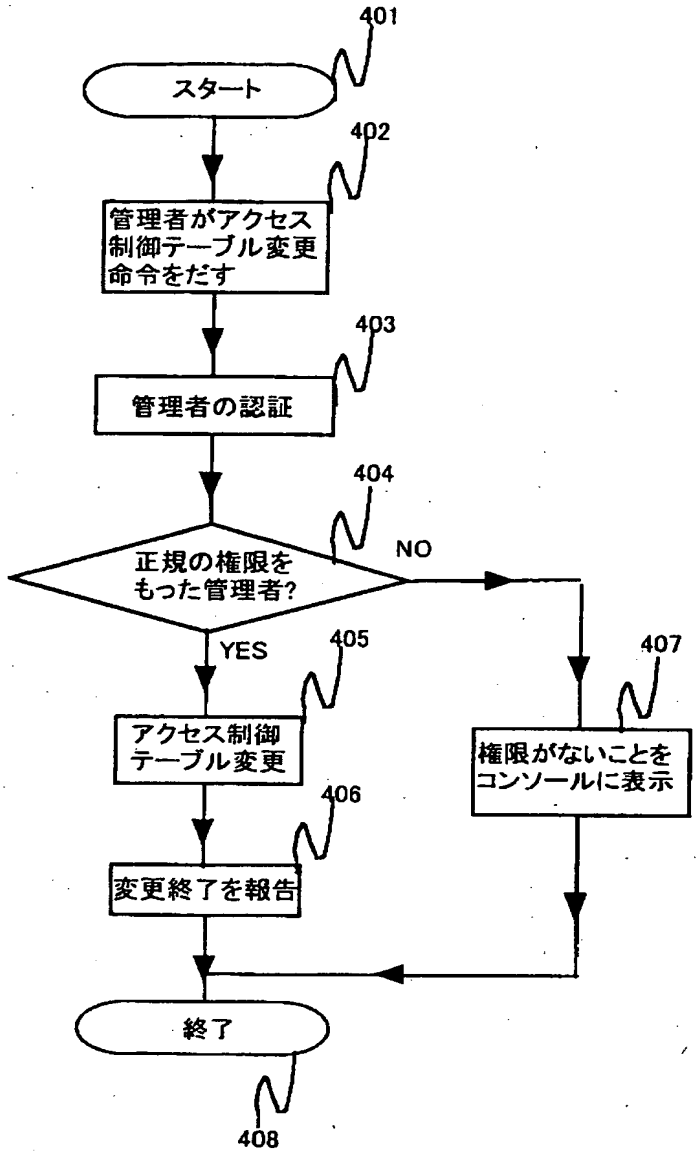


図3
301
スタート
302
入出力命令受信
303
論理ディスク識別子取得
通信ポート識別子取得
304
アクセス制御テーブル検索
305
当該命令は許可されている?
NO
YES
306
当該入出力命令を実行
307
当該入出力命令の失敗をホストコンピュータに送信
308
不正アクセスを管理コンソール124に報告
309
管理コンソール124は画面に表示し，管理者に通知
310
終了

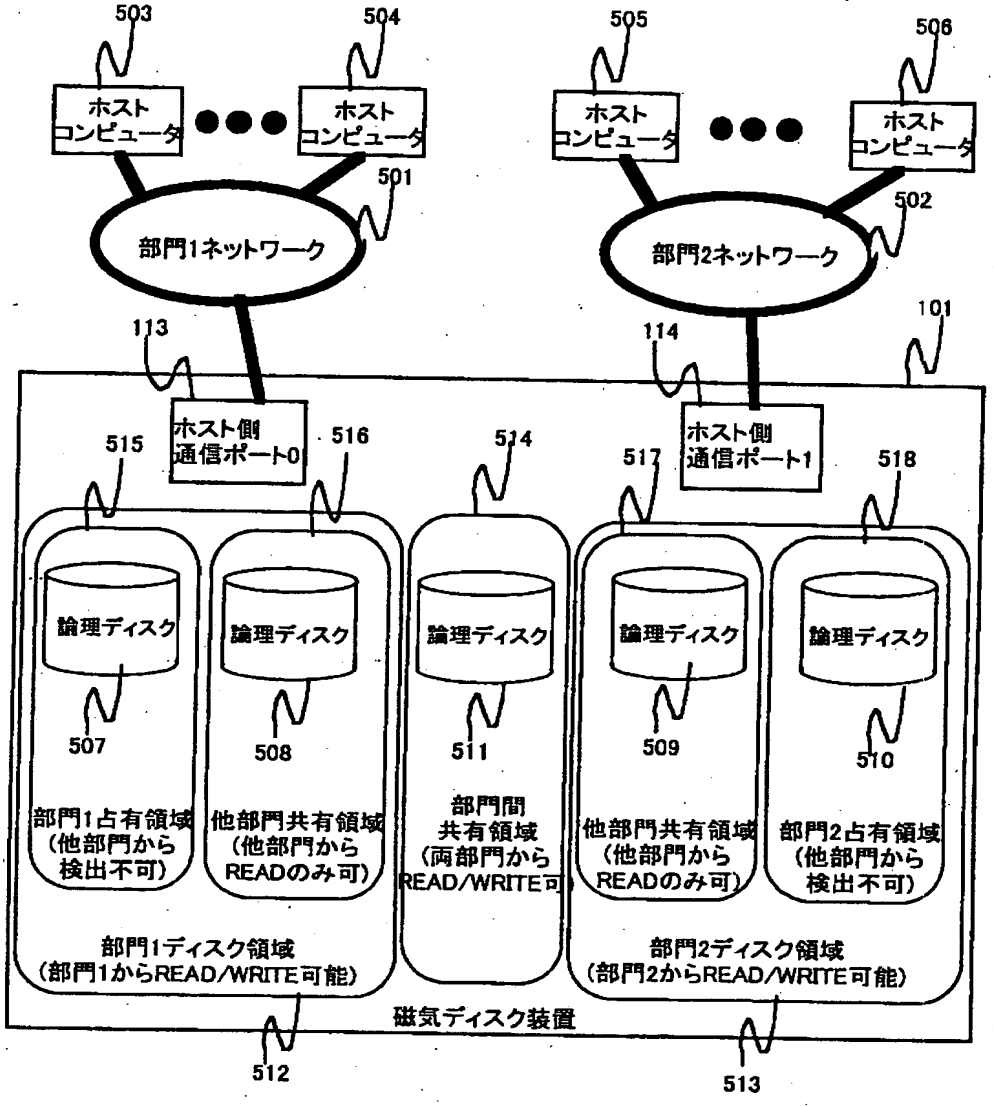
【図４】

図4


401
スタート
402
管理者がアクセス制御テーブル変更命令をだす
403
管理者の認証
404
正規の権限をもった管理者?
NO
YES
405
アクセス制御テーブル変更
406
変更終了を報告
407
権限がないことをコンソールに表示
終了
408

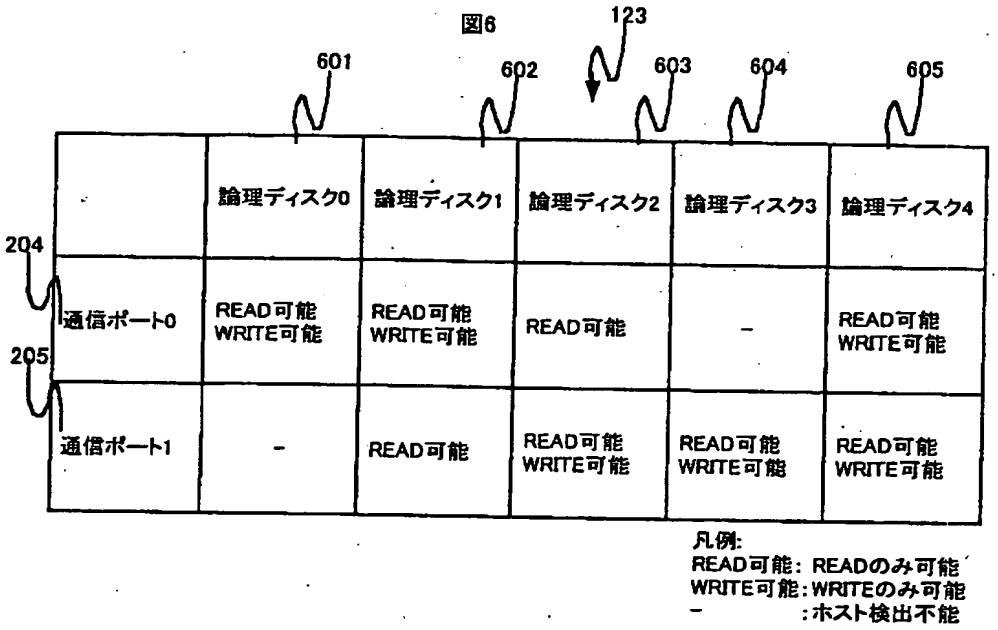
【図５】

図5


503
504
505
506
ホスト
コンピュータ
ホスト
コンピュータ
ホスト
コンピュータ
ホスト
コンピュータ
501
502
部門1ネットワーク
部門2ネットワーク
113
114
101
ホスト側
通信ポート0
ホスト側
通信ポート1
515
516
514
517
518
論理ディスク
論理ディスク
論理ディスク
論理ディスク
論理ディスク
507
508
511
509
510
部門1占有領域
(他部門から
検出不可)
他部門共有領域
(他部門から
READのみ可)
部門間
共有領域
(両部門から
READ/WRITE可)
他部門共有領域
(他部門から
READのみ可)
部門2占有領域
(他部門から
検出不可)
部門1ディスク領域
(部門1からREAD/WRITE可能)
部門2ディスク領域
(部門2からREAD/WRITE可能)
磁気ディスク装置
512
513

【図６】

図6



凡例:
READ可能: READのみ可能
WRITE可能: WRITEのみ可能
－ :ホスト検出不能

【図７】

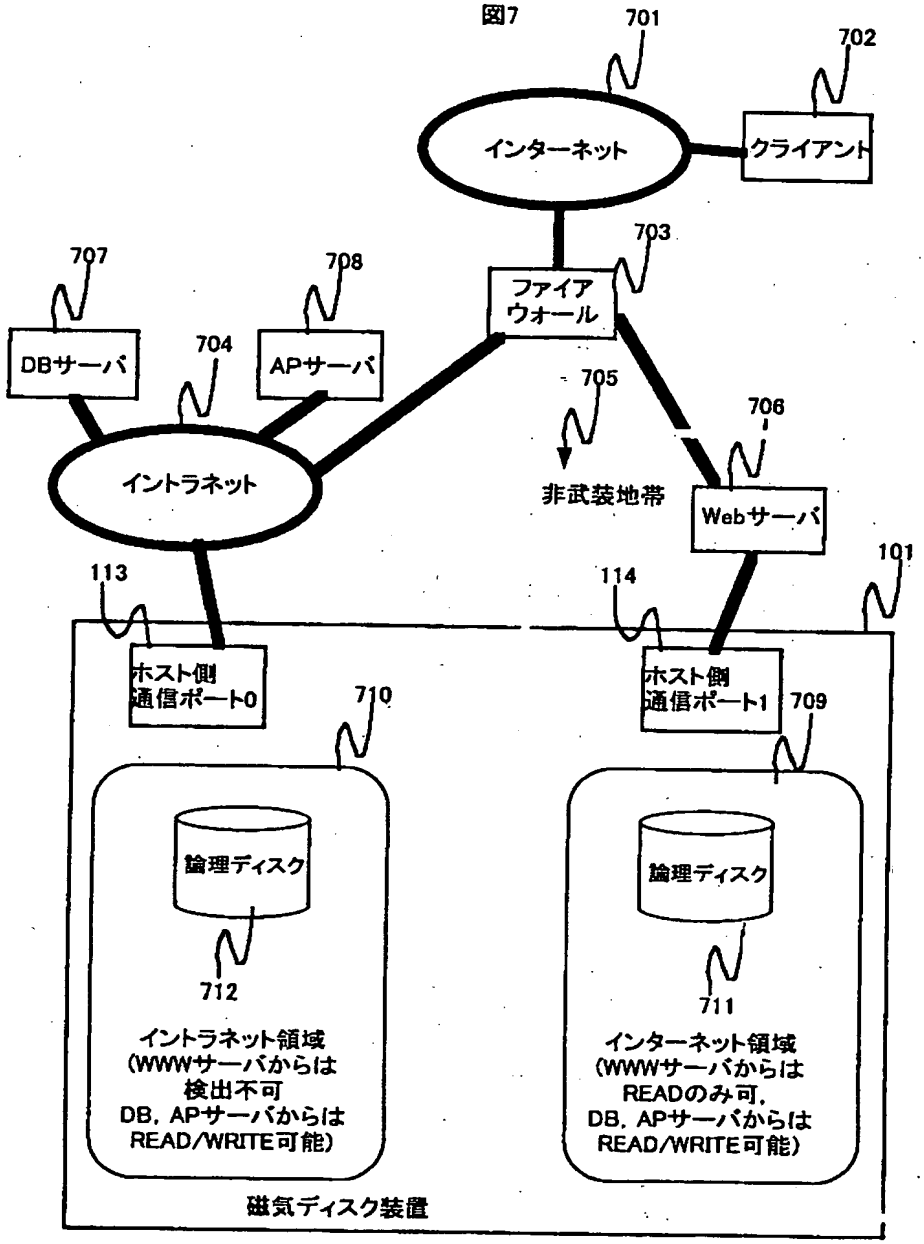
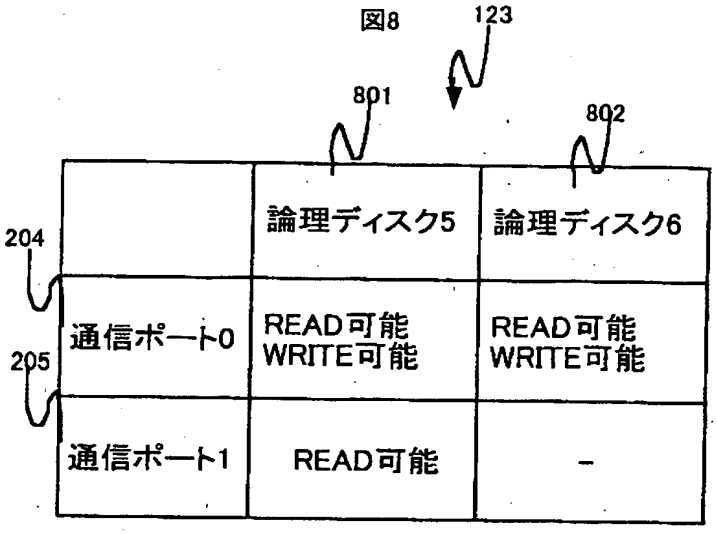


図7
701
702
インターネット
クライアント
703
ファイア
ウォール
707
708
DBサーバ
704
APサーバ
705
706
非武装地帯
Webサーバ
イントラネット
101
113
114
ホスト側
通信ポート0
ホスト側
通信ポート1
710
709
論理ディスク
論理ディスク
712
711
イントラネット領域
(WWWサーバからは
検出不可
DB，APサーバからは
READ/WRITE可能)
インターネット領域
(WWWサーバからは
READのみ可，
DB，APサーバからは
READ/WRITE可能)
磁気ディスク装置

【図８】

図8



凡例:
READ可能: READのみ可能
WRITE可能:WRITEのみ可能
- :ホスト検出不能

【書類名】要約書

【要約】

【課題】従来は、二次記憶装置側でホストコンピュータを認証していたが、成りすまし攻撃に弱かった。また、接続許可、拒否の2通りのオプションしか持っていないので、ホストコンピュータへの侵入が二次記憶装置内データの破壊に直結していた。

【解決手段】複数のネットワーク通信ポートを持ち、それぞれ異なるネットワークに接続し、通信ポートに対して二次記憶装置内データのアクセス権限を設定。さらに、入出力命令ごとに、許可、不許可を設定できるようにする。

【選択図】図１

認定・付加情報

特許出願の番号	特願２００２－００２９３５
受付番号	５０２０００２０３５４
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１４年　１月１１日

＜認定情報・付加情報＞

【提出日】　平成14年 1月10日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所